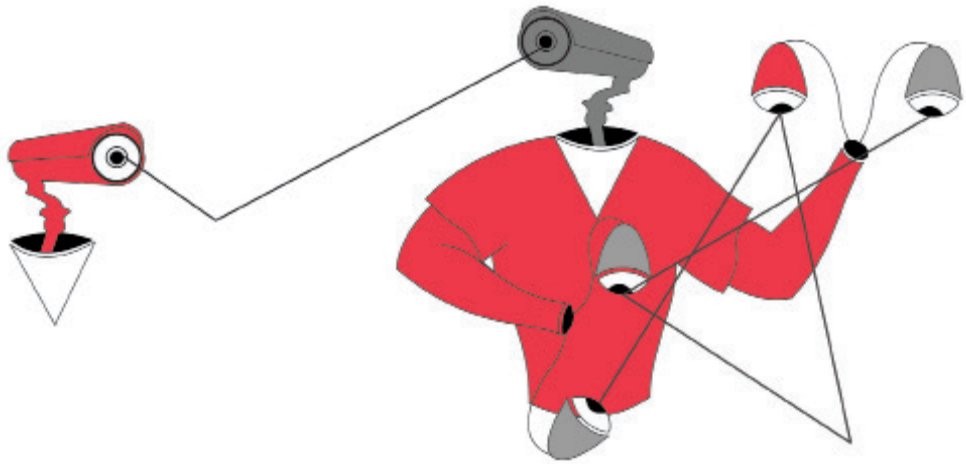
۲۰۱۶: سال هشیاری سازش‌پذیر



ترجمه: امیرهادی معنوی‌مقدم
T. Pendergast[1]

این مقاله که در سال ۲۰۱۶ تهیه شده است، به موضوع هشیاری سازش‌پذیر می‌پردازد.

امروز همه کسانی که در حوزه امنیت سایبری یا حوزه‌های نزدیک به آن فعالیت می‌کنند. تأثیر **چارچوب امنیت سایبریِ**[2] تدوین‌شده به‌وسیله **مؤسسه ملی استانداردها و فناوری**[3] را احساس کرده‌اند. این چارچوب منسجم به‌منظور تضمین حفاظت سازمانها در برابر به خطر افتادن امنیت اطلاعات می‌باشد؛ خطری که این روزها بسیار شایع است. نکته جالب‌توجهی که از این چارچوب به‌دست آمد- به‌ویژه برای کسانی که در فضای هشیاری هستند- مشکل سازمانها برای ایجاد برنامه سازش‌پذیر لایه ۴ است. برنامه «سازش‌پذیر» بر آموخته‌های قبلی و شاخصهای پیش‌بینی‌کننده مبتنی است.

این برنامه فرایند بهبود مستمر و سازش‌پذیری فعال برای مبارزه با تهدیدهای در حال تحول را دربر می‌گیرد و از سازمانها می‌خواهد تا برنامه‌ای برای هشیاری تدوین کنند؛ برنامه‌ای که به بخشی از فرهنگ سازمانی تبدیل خواهد شد.

کسانی که تلاش کرده‌اند برنامه‌ای مستمر برای آموزش امنیت سایبری اجرا کنند، به این مسئله آگاهی دارند که چنین برنامه‌ای چه مشکلهایی به بار خواهد آورد. آموزش امنیت سایبری باید برنامه‌ای بسیار انعطاف‌پذیر و ملموس باشد که بتواند در تاروپود فرهنگ سازمانی تنیده شود. به‌منظور ایجاد چنین برنامه‌ای، برخی شرکتهای فعال در این حوزه، در حد توان خود به کمک سازمانها آمده‌اند. اما آیا به‌واقع از پس این کار برخواهند آمد؟ در سال ۲۰۱۵، تعدادی از این شرکتها برای

ارائه برنامه‌های هشـیاری سازش‌پذیر که با این چارچوب در یک راستا باشـند، تواناییهای خود را ارتقا دادند. شاید سال ۲۰۱۶ سالی باشد که دریابیم سازمانها برای دستیابی به چنین سطح بالایی از آمادگی سازمانی، به چه چیزهایی نیاز دارند.

در همان حال که در فکر هستیم عناصر لازم احتمالی برای تدوین چنین برنامه‌ای چیست، مواردی نیز وجود دارند که باید آنها را زیر نظر داشته باشیم.

سازمانها تا چه اندازه ریسکشان را درک می‌کنند؟

هر سـازمانی، برای خلق برنامه هشـیاری در راستای ریسک واقعی خود، باید داده‌هایی را درباره عوامل ریسک جمع‌آوری کند (چیزی خلاف آن که فرض کند ریسـکش مانند ریسـک دیگر سازمانهاسـت و در نتیجه، برنامه‌ای مشابه ایجاد کند). برای درک ریسـک، ابزار زیادی وجود دارد که بسیاری از آنها دارای ماهیتی فنی هسـتند (به سازمانها کمک می‌کنند تا نقاط ضعف فنی‌شـان را درک کنند). کلیدِ برنامه‌های هشیاری (که تأثیر کارکنان و رفتارشـان بر امنیت سایبری را مورد توجه قرار می‌دهند)، این اسـت که معیارهای ریسکهای انسان‌محور را کشف کنند.

ارزیابی خوب و جامع ریسـک، برخی از این عوامل ریسک را مشـخص خواهد کـرد؛ اما سـازمانها باید مـواردی مانند برنامه‌های شبیه‌سازی دستبرد به اطلاعات شخصی (با هدف شناسـایی احتمال ریسـک مخرب مرتبط با عملیات دستبرد بـه اطلاعات شـخصی)، دیگر شبیه‌سـازی‌های مهندسـی اجتماعی، و ارزیابی دانش (با هدف شناسـایی دانش کنونی در جامعه کارکنان) را در نظر بگیرند. اسـتفاده از این موارد در کنار ارزیابی ریسـک تا حد زیادی ریسک سـازمان را به‌طور دقیق توضیح می‌دهد.

مورد دیگری که بیشـتر کارشناسان امنیت سایبری انتظار دارنـد طی یکی دو سـال آینده به این حوزه اضافه شـود، قابلیت یکپارچه‌سـازی رهیافتهای انسان‌محوری است که از ابزار فنی مختلف کنونی به‌دسـت می‌آینـد؛ برنامه‌هایی مانند **سـامانه‌های امنیتی مدیریت رویداد اطلاعات**[۴]، نرم‌افزار **جلوگیری از اتلاف داده‌ها**[۵]، گزارشـگری رویداد و **تحلیل رفتـار کاربر**[۶]. با وجود اینکه تمرکـز این ابزار بر شناسایی نقاط آسیب‌پذیر سامانه یا شناسایی و خنثی‌سازی ریسـکهای خارجی بوده است، اما باید انتظار داشت که آنها به‌گونه‌ای تکامل یابند تا درباره ریسکی که اقدامهای عمدی یا غیرعمـدی کارکنان برای امنیـت دارد، اطلاعات واقعی بدهند.

هدف از درک این عوامل ریسـک، صرفنظر از اینکه چه ابزاری برای درک آنها اسـتفاده شود، ایجاد تصویری دقیق از ریسک اسـت تا سازمان بتواند برای مقابله با آن ریسک، برنامه هشـیاری تدوین کند. بهتر است با این کار فهرستی هدفمند از ۵ تا ۱۰ عامل ریسـک انسان‌محور تهیه شود که بتوان به‌وسـیله آموزش و اطلاع‌رسـانی، آنها را پاسخ داد و دوره‌های اثربخشی‌شان را اندازه‌گیری کرد.

سازمانها برای اجرای چنین برنامه‌ای چه ظرفیتی دارند؟

چنانچه سـازمانی برای مقابله با ریسـک طرحی داشته باشد، مسـئله دیگری را نیز که باید در نظر بگیـرد، ظرفیتش برای اجـرای برنامه اسـت. در این‌بـاره صعود به قله کـوه، قیاس مفیدی است. چنانچه کوهی را که می‌خواهید به قله آن صعود کنید انتخاب کرده‌اید (برای نمونه، کوه دماوند)، در مرحله بعد باید از خودتان بپرسـید برای این صعـود چقدر آمادگی دارید؟ آیـا زمانی را برای آموزش و سـپس صعود بـه آن کوه در نظر گرفته‌اید؟ آیا هم‌نوردانتان را مشخص کرده‌اید (و آنها می‌دانند که قرار اسـت چه کاری را انجام دهیـد)؟ آیا تجهیزات لازم را دارید؟ همه اینها ملاحظه‌های مهمی اسـت که نباید دست‌کم گرفته شوند.

به‌طور مشابه، هنگام اجرای برنامه هشیاری، سازمانها باید موارد زیر را در نظر بگیرند:

- آیا سـازمان حمایـت و منابـع لازم برای ارائه آموزشـهای ضروری به‌صورت **برخط**[۷] را دارد؟
- اگر پاسخ آری است؛ آیا محدودیت زمانی خاص یا محدودیتهای دیگری هم برای آموزش دارد؟
- آیا سازمان ظرفیت و اجازه ارائه دیگر منابع (مانند ویدئو، بازی و پوسـترها) را بـرای تمامی کارکنان

دارد؟

- آیا مدیران اجرایی سازمان از این برنامه حمایت می‌کنند و این پیام را به اطلاع دیگران می‌رسانند؟
- آیا سازمان برای کمک به اجرای این برنامه، کارکنان کافی در اختیار دارد؟

سازمانها برای تدوین برنامه مقابله با ریسک، باید پاسخ پرسشهای پیش‌گفته (یعنی ظرفیت سازمان برای اجرای برنامه) را بدانند. ظرفیت سازمان مشخص خواهد کرد که آیا سازمان تنها نسبت به برگزاری یک کلاس آموزشی ضروری اقدام می‌کند یا اینکه طی سال و از طریق کارزار پایدار نمایش پوستر، بازیها و تصاویر متحرک، و الگوسازی دستبرد به اطلاعات و غیره، نسبت به ایجاد فرهنگ هشیاری از ریسک مبادرت خواهد ورزید.

سازمانها چگونه انعطاف‌پذیری لازم برای ارائه محتوای مناسب به افراد مناسب را پیدا می‌کنند؟

حتی اگر سازمانی حوزه ریسک خود را بشناسد و ظرفیت اجرای برنامه را نیز داشته باشد، یکی از بزرگ‌ترین مشکلات پیش‌رو، پیدا کردن یک مجموعه محتوای جذاب برای آموزش ریسک سازمانها به کارکنان و سپس سازش‌پذیرساختن آن با تغییرهای عوامل ریسک در گذر زمان است.

قابلیت سازش‌پذیری محتوا برای سازمانهایی که در پی ایجاد برنامه لایه ۴ هستند، بزرگ‌ترین مشکل را پیش می‌آورد. سازمانی که به سوی برنامه لایه ۴ می‌رود، به مجموعه‌ای از محتواهای مختلف و بسیار منعطفی نیاز دارد که با نیازهای کارکنان مطابقت داشته باشد و بتوان آن را به تفکیک وظایف کارکنان ارائه داد. این قابلیت از آنرو ضروری است که کارکنان با وظایف مختلف، به آموزشهای متفاوتی نیاز دارند.

برای نمونه، آموزش کارکنان امور مالی با آموزش کارکنان منابع انسانی از اساس متفاوت است و سازمان باید توانایی تغییر محتوا در پاسخ به ریسکهای جدید یا نوپدید را که بی‌شک طی سال تغییر خواهند کرد، داشته باشد. به همین دلیل، محتوای ثابت کارساز نبوده و با چشم‌انداز فعلی مطابقت ندارد.

نتیجه‌گیری

برای دستیابی به جایگاه لایه ۴ طبق چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری، سازمانها باید ریسکشان را درک کرده و ظرفیت ارائه آموزشهای ضروری و انعطاف‌پذیری لازم برای ارائه آموزش مناسب به افراد مناسب را داشته باشند. ریسکها دور نخواهند شد و به‌رغم نهایت تلاشهای کارشناسان امنیت اطلاعات، کارکنان همچنان نقش مهمی در نقض امنیت دارند. سازمانها و کارکنانشان همواره باید با ریسکهای جدید و نوپدید سازش پیدا کنند و بهترین راه برای این کار، تدوین برنامه هشیاری سازش‌پذیر است.

پانوشتها:

۱- دکتر **تام پندرگست** (Tom Pendergast)، معمار اصلی رویکرد معماری سازش‌پذیر در شرکت **مدیاپرو** (MediaPro)، برای برنامه‌ریزی، آموزش، تقویت و تحلیل یادگیری و هشیاری نیروی کار در زمینه امنیت اطلاعات، حریم خصوصی و رعایت مقررات شرکتی است. او نویسنده و ویراستار ۲۶ کتاب و مجموعه‌های مرجع است. دکتر پندرگست به‌عنوان بنیانگذار **فول سرکل ادیتوریال** (Full Circle Editorial)، در ابتدا تمامی زندگی حرفه‌ای خود را وقف طراحی محتوا و برنامه درسی به‌صورت چاپی و سپس آموزش راه‌کارها در شرکت مدیاپرو کرده است.

2- Cybersecurity Framework

3- National Institute of Standards and Technology (NIST)

4- Security Information Event Management Systems (SIEMSs)

5- Data Loss Prevention (DLP)

6- User Behavior Analytics (UBA)

7- Online

منبع:

Pendergast T., **The Year for Adaptive Awareness**, www.isaca.org, 2016